CHAPTER

# 9

# MANAGING GROUPS, FOLDERS, FILES, AND OBJECT SECURITY

**After reading this chapter and completing the exercises you will be able to:**

- Set up groups, including local, domain local, global, and universal groups, and convert Windows NT groups to Windows 2000 groups
- Manage objects, such as folders, through user rights, attributes, permissions, share permissions, auditing, and Web permissions
- Troubleshoot a security conflict
- Determine how creating, moving, and copying folders and files affect security

Windows 2000 Server contains many new features that enable it to excel in delivering file services—the services that your organization's clients use to access shared folders and files, such as documents, spreadsheets, databases, and software. Microsoft has significantly enhanced Windows 2000 Server to provide you with all kinds of ways to share resources while at the same time thoroughly securing them to match your organization's individual requirements. One of the best techniques for managing and securing shared resources, such as folders and files, is to use the different kinds of groups available in Windows 2000 Server. Complementing the use of groups are security measures that include an expanded range of rights and permissions. Windows 2000 Server also has a new option that enables you to use the **Encrypting File System** (**EFS**) to secure NTFS folders and files. EFS is a file encryption technique that guards information so that no one but the person who encrypts it can read it.

In this chapter you learn about the types of security groups offered through Windows 2000 Server and how to set up groups. You also learn how to use groups to manage object security, particularly folder and file security. In the process you learn about security descriptors that include user rights, attributes, permissions, auditing, and ownership. All of these tools enable you to offer folder and file resources to clients, while optimizing techniques to manage and secure those resources.

## Managing Server Resources and Security Through Groups

There are three ways administrators can manage domain resources and user accounts:

- By individual user
- By resource
- By group

Managing by individual user is the most labor-intensive method. This requires customizing security access for each user account. In an organization of 20 users, creating and managing individual accounts is not unmanageable, but can be time-consuming. On a network of 200 users, managing resources by individual account quickly becomes a nightmare. Another way to manage network access is by resource. Assume that resources on a network are two file servers and one print server. One file server is for business applications and one is for scientific research applications. The business unit in the organization would have access to the business applications server and the print server. Scientists would have access to the science-related server and the print server. Some managerial people would have access to all resources. The problem with this security model is that managing access is still labor-intensive because it is customized by user and by resource.

The group management concept saves time by eliminating repetitive steps in managing user and resource access. Windows 2000 Server expands on the concept of groups from the one used in Windows NT Server. In Windows NT Server there are two types of groups: local groups that are used to manage resources on a single server or on servers in one domain, and global groups that are used to manage resources across multiple domains. With the introduction of the Active Directory, Windows 2000 Server expands the use of groups through the concept of **scope of influence** (or **scope**), which is the reach of a group for gaining access to resources in the Active Directory. When the Active Directory is not implemented, the scope of resources is limited to the standalone server, and only local groups are created. In contrast, the implementation of the Active Directory increases the scope from a local server or domain to all domains in a forest. (See Chapter 4 for a discussion of the different elements of the Active Directory.) The types of groups and their associated scopes are as follows:

- *Local:* Used on standalone servers that are not part of a domain. The scope of this type of group does not go beyond the local server on which it is defined.
- *Domain local:* Used when there is a single domain or used to manage resources in a particular domain so that global and universal groups can access those resources
- *Global:* Used to manage group accounts from the same domain so that those accounts can access resources in the same and in other domains
- *Universal:* Used to provide access to resources in any domain within a forest

All of these groups can be used for security or distribution groups (see Chapter 4). Security groups are used to enable access to resources on a standalone server or in the Active Directory. Distribution groups are used for e-mail or telephone lists, to provide quick, mass distribution of information. In this chapter, the focus is on security groups.

## Implementing Local Groups

A **local security group** is used to manage resources on a standalone computer that is not part of a domain. For example, you might use a local group in a small office situation in which there are only a few users, for example 5, 15, or 30. Consider an office of mineral resource consultants in which there are 18 user accounts on the server. Four of these accounts are used by the founding partners of the consulting firm, who manage employee hiring, payroll, schedules, and general accounting. Seven accounts are for consultants who specialize in coal-bed methane extraction, and the seven remaining accounts belong to consultants who work with oil extraction. In this situation, the company may decide not to install the Active Directory, and divide these accounts into three local groups. One group would be called Managers and consist of the four founding partners. Another group would be called CBM for the coal-bed methane consultants, and the third group would be called Oil and used for the oil consultants. Each group would be given different security access based on the resources at the server, which would include access to folders and to printers.

## Implementing Domain Local Groups



A **domain local security group** is used when the Active Directory is deployed. This type of group is typically used to manage resources in a domain and to give global groups from the same and other domains access to those resources. As shown in Table 9-1, a domain local group can contain members such as global groups, and it can be a member of access control lists (ACLs; see Chapter 4) and other domain local groups.

**Table 9-1** Membership Capabilities of a Domain Local Group

| Active Directory Objects That Can Be Members of a Domain Local Group | Active Directory Objects That a Domain Local Group Can Join as a Member |
|---|---|
| User accounts in the same domain | Access control lists for objects in the same domain, such as permissions to access a folder, shared folder, or printer |
| Domain local groups in the same domain | Domain local groups in the same domain |
| Global groups in any domain in a tree or forest (as long as there are transitive or two-way trust relationships maintained) | |
| Universal groups in any domain in a tree or forest (as long as there are transitive or two-way trust relationships maintained) | |

The scope of a domain local group is the domain in which the group exists, but you can convert a domain local group to a universal group as long as the domain local group does not contain any other domain local groups. Also, to convert any group, the domain must be in native mode and not mixed mode. **Native mode** means there are only Windows 2000 Server domain controllers. **Mixed mode** consists of Windows NT 4.0 domain controllers (PDC and BDCs) and Windows 2000 Server domain controllers (DCs) and is typically used

when an organization is in the process of converting from a Windows NT 4.0 Server environment to Windows 2000 Server.


Mixed mode is the default for all domains unless you change it to native mode to reflect that there are no Windows NT 4.0 servers in the domain. Once you change from mixed to native mode you cannot change back. Try Hands-on Project 9-1 to practice changing from mixed to native mode.

Although a domain local group can contain any combination of accounts, plus local, global, and universal groups, *the typical purpose of a domain local group is to provide access to resources*, which means that you grant access to servers, folders, shared folders, and printers to a domain local group. Under most circumstances you should plan to put domain local groups in access control lists only, and the members of domain local groups should be mainly global groups. Generally, a domain local group does not contain accounts, because account management is more efficient when you handle it through global groups. Examples of using domain local groups with global groups are presented in the next section.

## Implementing Global Groups

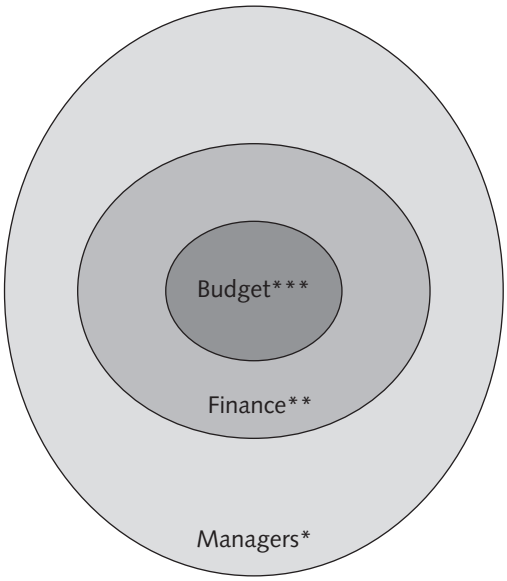
A **global security group** is intended to contain user accounts from a single domain and can also be set up as a member of a local group in the same or another domain (as long as the domain in which the global group is set up is trusted by the domain of the local group of which it becomes a member). This capability gives global groups a broader scope than domain local groups, because their members can access resources in other domains. Table 9-2 shows which Active Directory objects can be members of global groups and which objects global groups can join.

**Table 9-2** Membership Capabilities of a Global Group

| Active Directory Objects That Can Be Members of a Global Group | Active Directory Objects That a Global Group Can Join as a Member |
|---|---|
| User accounts from the domain in which the global group was created | Access control lists for objects in any domain in a forest (as long as a transitive trust is maintained between domains) |
| Other global groups that have been created in the same domain | Domain local groups in any domain in a forest |
| Levels of global groups, so that global groups can be nested to reflect the structure of organizational units (OUs) in a domain | Global groups in any domain in a forest |
| | Universal groups in a forest |

Nesting global groups to reflect the structure of OUs means that global groups can be layered. For example, your organization might consist of an OU for management, an OU under the management OU for the Finance department, and an OU under the Finance department

for the Budget office—resulting in three levels of OUs. Also, you might have a global group composed of the accounts of vice presidents in the management OU, a global group of accounts for supervisors in the Finance department OU, and a global group of all members of the Budget office in the budget OU. The global group membership can be set up to reflect the structure of OUs, as shown in Figure 9-1.




*Managers global group (top-level global group)
Amber Richards
Joe Scarpelli
Kathy Brown
Sam Rameriz
**Finance global group (second-level global group)
Martin LeDuc
Sarah Humphrey
Heather Shultz
Sam Weisenberg
Jason Lew
***Budget global group (third-level global group)
Michele Gomez
Kristin Beck
Chris Doyle

**Figure 9-1** Nested global groups


Plan nesting of global groups carefully. You can convert a global group to a universal group at a later time, but only if it is not a member of another global group. Also, global groups can only be nested in native mode domains.

A global group can be converted to a universal group as long as it is not nested in another global group or in a universal group. In the example shown in Figure 9-1, the Finance and Budget global groups cannot be converted to universal groups because they already are members of the Managers and Finance groups, respectively.

*A typical use for a global group is to build it with accounts that need access to resources in the same or in another domain and then to make the global group in one domain a member of a local group in the same or another domain.* This model enables you to manage user accounts and their access to resources through one or more global groups, while reducing the complexity of managing accounts.

For example, consider a college that has a domain for students, a domain for faculty and staff, and a domain for research organizations that are associated with the college. The college's executive council, consisting of the college president and vice presidents, needs access to resources in all three domains. One way to enable the executive council to have access is to create a domain local group called LocalExec in each domain that provides the appropriate access to folders, files, and other resources. Next, create a GlobalExec global group in the faculty and staff domain that has the president's and vice presidents' user accounts as members (see Figure 9-2). These steps enable you to manage security for all of their accounts at one time from one global group. If the president or a vice president leaves to take another job, you simply delete (or disable) that person's account from the global group and later add an account (or rename and enable the old account) for her or his replacement. You also can manage access to resources in each domain one time through each domain local group, resulting in much less management work. If a new printer is added to a domain, for example, you can give the domain local group full privileges to the printer. (Try Hands-on Project 9-2 to practice setting up a domain local group and a global group.)

When the Active Directory structure becomes complex enough in a large organization so that many domains, trees, and forests are in use, global groups are used as members of universal groups to manage accounts, as described in the next section.

## Implementing Universal Groups

In an Active Directory context in which there are multiple hierarchies of domains, trees, and forests, **universal security groups** provide a means to span domains and trees. These groups can have members and can join the Active Directory objects, as shown in Table 9-3.

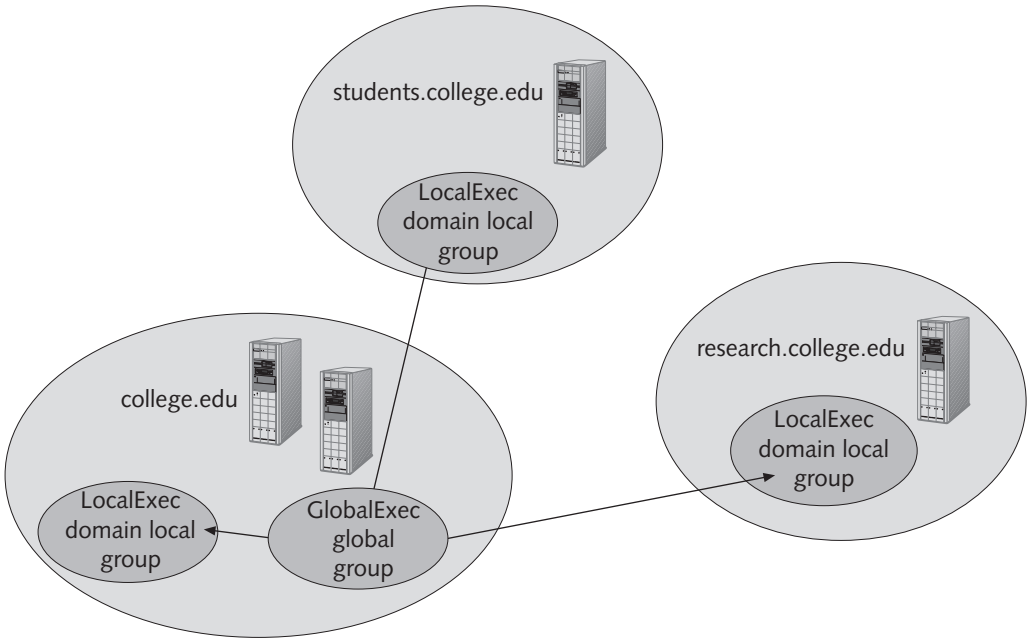



**Figure 9-2** Managing security through domain local and global groups

**Table 9-3** Membership Capabilities of a Universal Group

| Active Directory Objects That Can Be Members of a Universal Group | Active Directory Objects That a Universal Group Can Join as a Member |
|---|---|
| Accounts from any domain in a forest | Access control lists for objects in any domain in a forest |
| Global groups from any domain in a forest | Any domain local group in a forest |
| Universal groups from any domain in a forest | Any universal group in a forest |


A universal group can only be created in native mode (only Windows 2000 servers), not in mixed mode (a combination of Windows NT 4.0 and 2000 servers). Also, a universal group cannot be converted to a smaller scope, such as to a global or domain local group.

Universal groups are offered to provide an easy means to access any resource in a tree or among trees in a forest. If you carefully plan the use of universal groups, then you can manage security for single accounts with a minimum of effort. That planning is done in relation to the scope of access that is needed for a group of accounts. Here are some guidelines to help simplify how you plan to use groups:

- Use global groups to hold accounts as members—and keep the nesting of global groups to a minimum (or do not use nesting), to avoid confusion. Give accounts access to resources by making the global groups to which they belong members of domain local groups or universal groups or both.

- Use domain local groups to provide access to resources in a specific domain. Avoid placing accounts in domain local groups—but do make domain local groups members of ACLs for specific resources in the domain, such as shared folders and printers.
- Use universal groups to provide extensive access to resources, particularly when the Active Directory contains trees and forests, or to simplify access when there are multiple domains. *Make universal groups members of ACLs for objects in any domain, tree, or forest*. Manage user account access by placing accounts in global groups and joining global groups to domain local or universal groups, depending on which is most appropriate to the scope required for access.


If you attempt to create a new universal group, but find that the radio button in the Create New Object – (Group) dialog box is deactivated, this means that the domain is set up in mixed mode and you must convert the domain to native mode before you can create the group (see Hands-on Project 9-1).

In the example of setting up access for the executive council in a college that has three domains, an alternative is to create one universal group that has access to all resources in the three domains—create one global group containing the president and vice presidents, and make that global group a member of the universal group (see Figure 9-3). In this model there are only two groups to manage, compared to the model shown in Figure 9-2, in which there are four groups to manage.

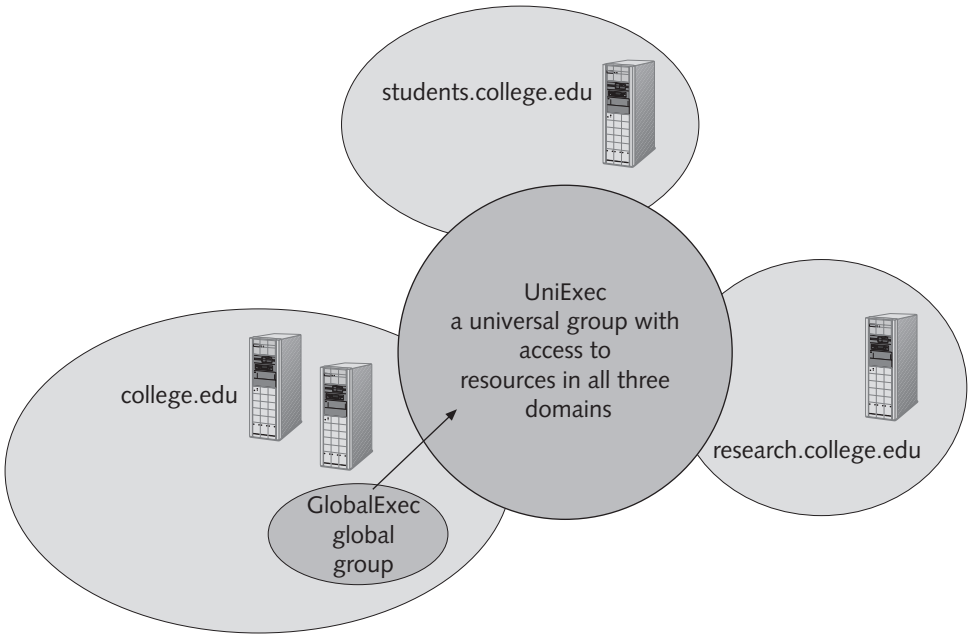



**Figure 9-3** Managing security through universal and global groups

## Creating Groups

Groups are created by using the Local Groups and Users tool when the Active Directory is not installed and by using the Active Directory Users and Computers tool when the Active Directory is installed. For example, to create a group using the Active Directory Users and Computers tool:

1. Click the container in which to create the group, such as the domain, the Users container (the default container of user accounts), or an OU within a domain.
2. Click the Action menu, point to New, and then click Group; or, click the *Create a new group in the current container* icon on the button bar.
3. Enter the name of the group in the Group name box (see Figure 9-4). A pre-Windows-2000 group name is also entered for use by Windows NT servers if you are running in mixed mode.
4. Click the group scope from the selections that are Domain local, Global, and Universal.
5. Click the group type, which is either Security or Distribution.
6. Click OK and verify that the group is displayed in the container you selected at the start.



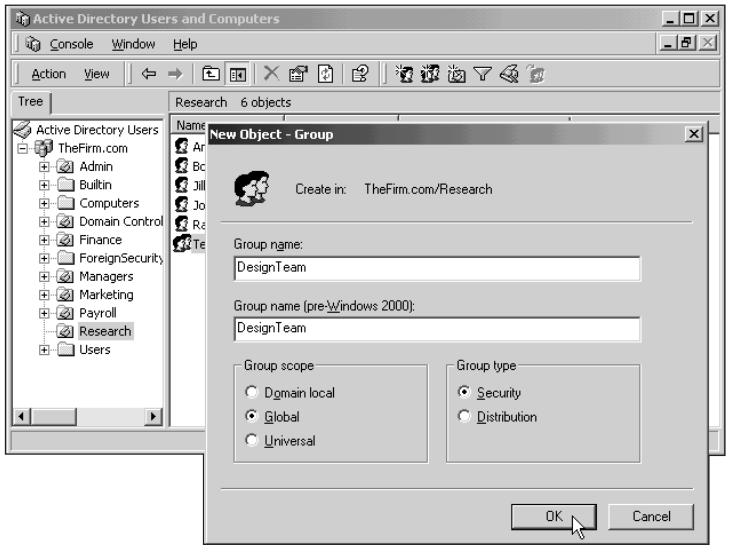



**Figure 9-4** Creating a group

Each group has an associated set of properties that can be modified after the group is created, for example to add user accounts to the group or to make the group a member of another group. You can access the properties by double-clicking the group after you create it, for

example in the Active Directory Users and Computers tool, where you will find the group under the container in which you created it. There are four tabs in the properties dialog box:

- *General:* Used to enter a description of the group, change the scope and type of group, and provide an e-mail address for a distribution group
- *Members:* Used to add members to a group, for example adding user accounts to a global group (click the Add button to add members; see Figure 9-5)
- *Member Of:* Used to make the group a member of another group (click the Add button to add the group to another group)
- *Managed By:* Used to establish an account or group that will manage the group, if the manager is other than the server administrator; also, the location, telephone number, and fax number of the manager can be provided

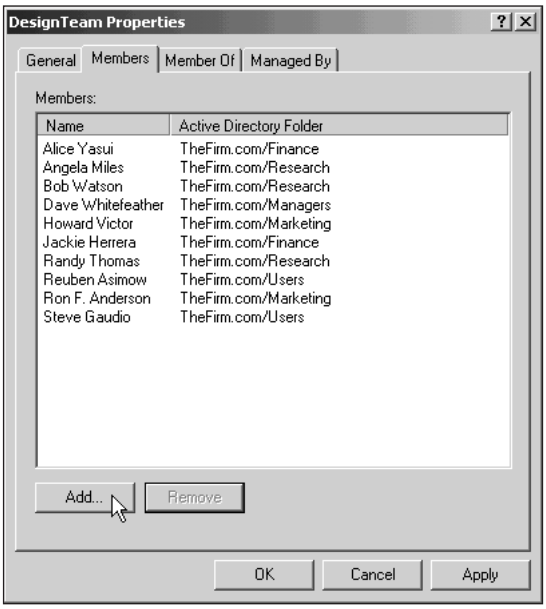



**Figure 9-5** Adding group members


The General tab enables you to change group scope, but only in the permitted direction. For example, you can change a global group into a universal group, but not into a domain local group. In this example, the domain local group will be deactivated so that you cannot select it. (Try Hands-on Project 9-3 to practice changing group scope.)

## Converting Groups from Windows NT Server

When you upgrade Windows NT Server to Windows 2000 Server, the existing NT local groups on a primary domain controller are automatically converted to domain local groups, and the NT global groups are converted to global groups. If you continue to run in mixed

mode because there are remaining Windows NT Server backup domain controllers, then the Windows NT servers recognize the converted groups as Windows NT local and global groups. A Windows NT server that does not run using Active Directory client software cannot recognize a universal group (see Chapter 8). With the Active Directory client installed, a Windows NT server treats a universal group as a Windows NT global group.

## Default Windows 2000 Groups

Windows 2000 Server comes with several predefined domain local, global, and universal groups when the Active Directory is installed. For example, there is always a global Domain Administrators group called Domain Admins that starts by having the Administrator account as a member. The predefined groups can vary, depending on which services are installed. For instance, a domain local DHCP Administrators group is set up when you set up a DHCP server, and you will likely want to be sure that the Domain Adminis global group is a member. Table 9-4 shows many examples of the predefined Windows 2000 Server groups. When the Active Directory is installed, these groups are found in one of two containers in a domain tree, Builtin or Users.




The Builtin group contains local (on a standalone server) or domain local (in the Active Directory) groups that are used to help manage the server, such as Backup Operators. If you have used Windows NT 4.0, you will find that these are the same default groups created by that operating system.

**Table 9-4** Windows 2000 Predefined Security Groups

| Security Group | Scope | Active Directory Container Location/Default Members | Description |
|---|---|---|---|
| Account Operators | Built-in local [1] | Builtin | Used for administration of user accounts and groups |
| Administrators | Built-in local [1] | Builtin/Administrator account; Domain Admins and Enterprise Admins groups | Provides complete access to all local computer and/or domain resources |
| Backup Operators | Built-in local [1] | Builtin | Enables members to back up any folders and files on the computer |
| Cert Publishers | Global [1] | Users | Used to manage enterprise certification services for security |
| DHCP Administrators | Domain local | Users/Domain Admins group | Used to manage the DHCP server services (when DHCP server services are installed) |

**Table 9-4** Windows 2000 Predefined Security Groups (continued)

| Security Group | Scope | Active Directory Container Location/Default Members | Description |
|---|---|---|---|
| DHCP Users | Domain local | Users | Enables users to access DHCP services when DHCP is enabled at the client (when DHCP server services are installed) |
| DNSAdmins | Domain local | Users | Used to manage the DNS server services (when DNS server services are installed) |
| DNSUpdateProxy | Global | Users | Enables each user access as an update proxy, so that a DHCP client can automatically update the DNS server information with its IP address |
| Domain Admins | Global [1] | Users/Administrator account | Used to manage resources in a domain |
| Domain Computers | Global [1] | Users | Used to manage all workstations and servers that join the domain |
| Domain Controllers | Global [1] | Users/all DC computers | Used to manage all domain controllers in a domain |
| Domain Guests | Global [1] | Users/Guest account | Used to manage all domain guest-type accounts, such as those for temporary employees |
| Domain Users | Global [1] | Users/all user accounts | Used to manage all domain user accounts |
| Enterprise Admins | Universal [1] | Users/Administrator account | Used to manage all resources in an enterprise |
| Everyone | Built-in local [1] | Does not appear in a container and cannot be deleted | Used to manage default access to local or domain resources; all user accounts are automatically members |
| Group Policy Creator Owners | Global [1] | Users/Administrator account | Enables members to manage group policy |
| Guests | Built-in local [1] | Builtin/Guest and IIS accounts, Domain Guests group | Used to manage guest accounts and to prevent access to install software or change system settings |

**Table 9-4** Windows 2000 Predefined Security Groups (continued)

| Security Group | Scope | Active Directory Container Location/Default Members | Description |
|---|---|---|---|
| Pre-Windows-2000 Compatible Access | Built-in local [1] | Builtin/pre-Windows-2000 Everyone group | Used for backward compatibility to the Everyone group on Windows NT servers; limits access to read |
| Print Operators | Built-in local [1] | Builtin | Members can manage printers on the local computer or in the domain |
| RAS and IAS Servers | Domain local [1] | Users | Enables member servers to have access to remote access properties that are associated with user accounts, such as security properties |
| Replicator | Built-in local [1] | Builtin | Used with the Windows File Replication service to replicate designated folders and files |
| SchemaAdmins | Universal [1] | Users/Administrator account | Members have access to modify schema in the Active Directory |
| Server Operators | Built-in local [1] | Builtin | Used for common day-to-day server management tasks |
| Users | Built-in local [1] | Builtin/Domain Users group | Used to manage general user access, including the ability to be authenticated as a user and to communicate interactively |

[1] The group scope cannot be changed



## Managing Objects and Object Security

The purpose in creating groups is to help you to manage objects on a local server and in the Active Directory. The objects you will manage through groups include disk volumes, folders, files, printers, software, program processes, and network services. Each of these objects has an ACL to which you can add a group, such as a domain local group, so that an object can be managed as a shared resource.

Access to objects is controlled through common security techniques that include user rights, permissions, inherited rights and permissions, ownership, share permissions, and Web sharing. User rights enable an account or group to perform predefined tasks in the domain. The

most basic right is the ability to access a server. More advanced rights give privileges to create accounts and manage server functions. There are two general categories of rights: privileges and logon rights. Privileges generally relate to the ability to manage server or Active Directory functions, and logon rights are related to how accounts, computers, and services are accessed. Table 9-5 shows the options included in each. Both types of rights are established through setting up the user rights group policy.

**Table 9-5** Rights Security

| Privileges | Logon Rights |
|---|---|
| Act as part of the operating system (a program process can gain security access as a user) | Access this computer from the network |
| Add workstations to a domain | Deny access to this computer from the network |
| Back up files and directories | Deny logon as a batch job |
| Bypass traverse checking (enables a user to move through a folder that the user has no permission to access, if it is on the route to one that she or he does have permission to access) | Deny logon as a service |
| Change the system time | Deny logon locally |
| Create a pagefile | Log on as a batch job |
| Create a token object (a process can create a security access token to use any local resource; normally should be reserved for administrators) | Log on as a service |
| Create permanent shared objects | Log on locally |
| Debug programs (can install and use a process debugger to trace problems; normally should be reserved for administrators) | |
| Enable computer and user accounts to be trusted for delegation | |
| Force shutdown from a remote system | |
| Generate security audits | |
| Increase quotas | |
| Increase scheduling priority | |
| Load and unload device drivers | |
| Lock pages in memory (included for backward compatibility with Windows NT and should not be used, because it degrades performance) | |
| Manage auditing and security log | |
| Modify firmware environment variables | |

**Table 9-5** Rights Security (continued)

| Privileges | Logon Rights |
|---|---|
| Profile single process (can monitor nonsystem processes) | |
| Profile system performance (can monitor system processes) | |
| Remove computer from docking station | |
| Replace a process-level token (enables a process to replace a security token on one or more of its subprocesses) | |
| Restore files and directories | |
| Shut down the system | |
| Synchronize directory service data | |
| Take ownership of files or other objects | |



The most efficient way to assign user rights is to assign them to groups instead of to individual user accounts. When user rights are assigned to a group, then all user accounts (or groups) that are members of that group inherit the user rights assigned to the group, making these **inherited rights**.

Permissions are associated with folders and files, controlling the way an account or group accesses information. For example, access can range from no permission to view files in a folder to full permission to add or change any files in the folder. User rights are a higher level of access than permissions. For instance, if the server administrator gives an account permission to access all software application files on the server but does not grant that account rights to access the server, the account cannot access the applications.

**Share permissions** are special permissions that apply to a particular shared object, such as a shared folder or printer. Share permissions do not offer as many options as user rights and regular permissions, in part because they are matched to the characteristics of the shared object, such as the ability to manage print jobs on a shared printer.

In general, rights, permissions, and share permissions are cumulative. This means that a user account, for example, has all of the rights and permissions of all of the groups to which it belongs. There are two primary exceptions to this rule: (1) a right or permission can be specifically denied and (2) the Administrators group always has the means to gain access to any resource. For example, if a user's account belongs to one group that has Full Control access to a folder and to another group that is denied access entirely, then that account will have no access.

## Configuring Rights

You can configure rights as a group policy. You can start with configuring rights in the default group policy for a domain. If you need to customize rights for OUs in the domain, you can do that by setting up a group policy for specific OUs. A fast way to access the group

policy for a domain or OU and to set user rights is as follows (also try Hands-on Project 9-4 to practice setting user rights in a group policy):

1. Open the Active Directory Users and Computers tool.
2. Right-click the domain or OU in the Console tree.
3. Click Properties and then click the Group Policy tab.
4. Click the group policy under Group Policy Object Links, and click Edit.
5. As necessary to expand the view in the tree, double-click Windows Settings under Computer Configuration, double-click Security Settings, and double-click Local Policies.
6. Double-click User Rights Assignment.
7. Double-click any of the policies in the right pane to configure it (see Figure 9-6).

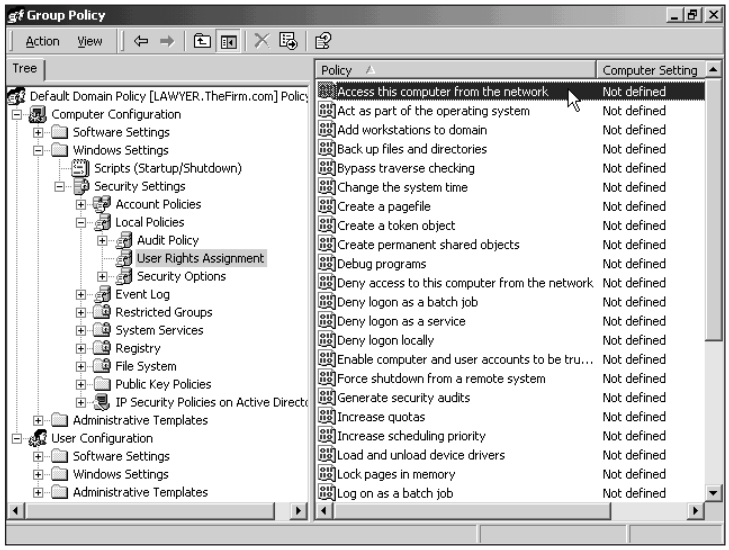



**Figure 9-6** Configuring user rights as part of group policy

## Configuring Folder and File Security

There are three types of security associated with Windows 2000 folders and files on a FAT-formatted drive: attributes, share permissions, and Web permissions. Folders and files on an NTFS-formatted drive have much tighter security because three additional measures are added: permissions, auditing, and ownership.


Always set up or check folder security before releasing a new server or folder on a server for public access.

## Configuring Attributes

Use of **attributes** is retained in FAT and NTFS as a carryover from earlier DOS-based systems and to provide a partial migration path to convert files and directories from a Novell NetWare file server. DOS and NetWare systems use file attributes as a form of security and file management. Attributes are stored as header information with each folder and file, along with other characteristics, including volume label, designation as a subfolder, date of creation, and time of creation.

The folder and file attributes available in a FAT-formatted Windows 2000 Server disk are Read-only, Hidden, and Archive and are accessed from the General tab when you right-click a folder or file and click Properties (see Figure 9-7). If you check Read-only for a folder, the folder is read-only, but not the files in the folder. This means that the folder cannot be deleted or renamed from the Command Prompt. Also, it can only be deleted or renamed by a user belonging to the Administrators group. If an administrator attempts to delete or rename the folder, a warning message states that the folder is read-only and asks whether to proceed. Most Windows 2000 server administrators leave the read-only box blank and set the equivalent protection in permissions instead, because the read-only *permissions* apply to the folder and can be inherited by its files.



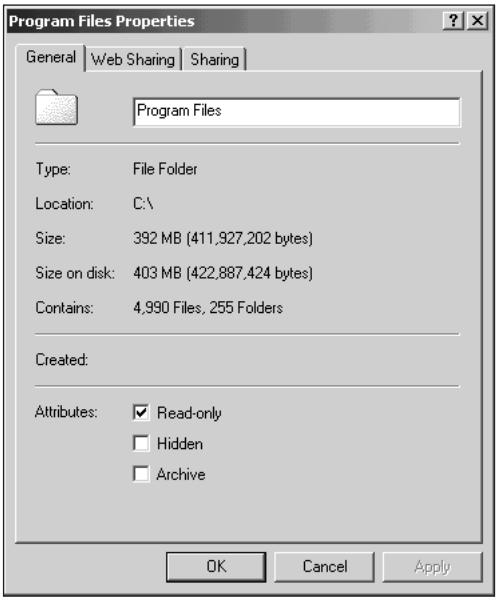



**Figure 9-7** Attributes of a folder on a FAT-formatted disk

Folders can be marked as Hidden to prevent users from viewing their contents. For example, one college server administrator placed zip code verification software on a network, but kept the folder hidden while several users tested it. After testing was completed, the Hidden attribute was removed.


The Hidden attribute can be defeated in Windows 95, Windows 98, Windows NT, and Windows 2000 by selecting the option to view hidden files and folders from the View or Tools menu (depending on the version of Windows) in Windows Explorer or My Computer.

The Archive attribute is checked to indicate that the folder or file needs to be backed up, because the folder or file is new or changed. Most network administrators ignore the folder Archive attribute, but instead rely on it for files. Files, but not folders, are automatically flagged to archive when they are changed. File server backup systems can be set to detect files with the Archive attribute, to ensure that those files are backed up (see Chapter 7). The backup system ensures that each file is saved, following the same folder or subfolder scheme as on the server.

An NTFS volume has the Read-only, Hidden, and Archive attributes plus the Index, Compress, and Encrypt attributes. The Read-only and Hidden attributes are on the General tab in an NTFS folder's or file's properties dialog box, and the other attributes, called extended attributes, are accessed by clicking the General tab's Advanced button (see Figure 9-8). When you make a change to one of the attributes in the Advanced Attributes dialog box in a folder's properties, you have the option to apply that change to only the folder and the files in that folder or to the folder, its files, and all subfolders and files within the folder (make sure you click the Apply button when you return to the General tab).

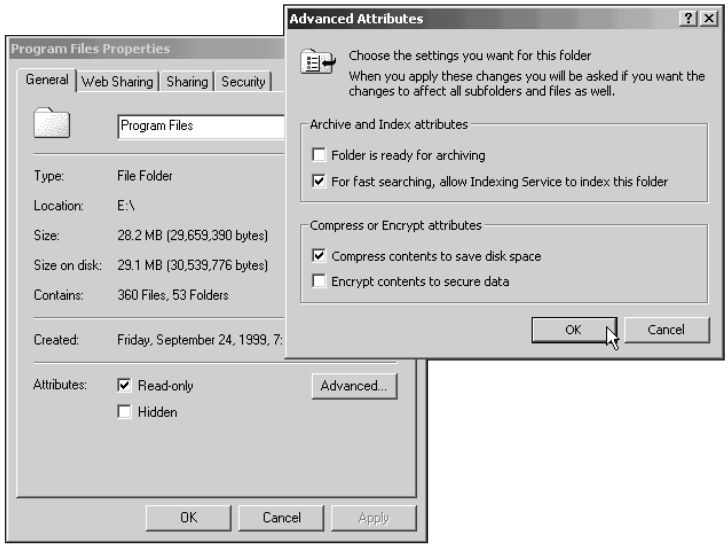



**Figure 9-8** Attributes of a folder on an NTFS-formatted disk

The Index attribute is used to index the folder and file contents so that text, creation date, and other properties can be quickly searched in Windows 2000, using the Search button in My Computer or Windows Explorer.

The Index attribute relies on two preliminary steps in order to work. The first step is that the Indexing Service must already be installed as a Windows 2000 component (see Chapter 6). Also, the service should be set to start automatically after it is installed by clicking Start, pointing to Programs, pointing to Administrative Tools, clicking Computer Management, double-clicking Services and Applications in the left pane, clicking Services in the left pane, double-clicking Indexing Service in the right pane, and setting the Startup type box to Automatic.

A folder and its contents can be stored on the disk in compressed format, which is an option that enables you to save on the amount of disk space used for files, particularly in situations in which disk space is limited or for directories that are accessed infrequently, such as those used to store old fiscal year accounting data. Compression saves space, but it takes longer to access compressed information because each file must be decompressed before it is read.

If you are concerned about security and want to use the Encrypt attribute, do not compress files, because compressed files cannot be encrypted.



The Encrypt attribute protects folders and files so that only the user who encrypts the folder or file is able to read it. As administrator, you might use this option to protect certain system files or new software files that you are not yet ready to release for general use (try Hands-on Project 9-5 to encrypt the contents of a folder).

An encrypted folder or file uses Microsoft's Encrypting File System (EFS), which sets up a unique private encryption key that is associated with the user account that encrypted the folder or file. The file is protected from network intruders and situations in which a server or hard drive is stolen. When you move an encrypted file to another folder, that file remains encrypted, even if you also rename it. You can decrypt a folder or file by using Windows Explorer or My Computer to remove the Encrypt attribute and then applying the change. Folders and files can also be encrypted or decrypted by using the Command Prompt's *cipher* command. (Click Start, point to Programs, point to Accessories, and click Command Prompt. Type *cipher /?* in the Command Prompt window to view the command's switch options.)

## Configuring Additional Security Options

Click the Security tab and use the Advanced button on an NTFS folder's properties dialog box to set up additional security that includes permissions, auditing, and ownership (see Figure 9-9). **Permissions** control access to the folder and its contents. **Auditing** enables the administrator to audit activities on a folder or file, such as the number of times the folder or file has been read or changed. **Ownership** designates the folder owner who has the ability to change permissions, share permissions, and Web sharing for that folder.

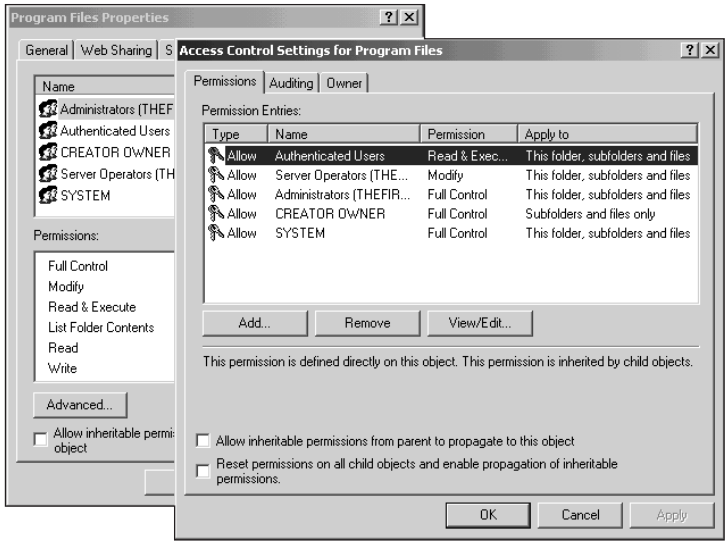



**Figure 9-9** Configuring security options


Permissions can be set on individual files within a folder. However, managing these exceptions can become time-consuming and confusing. Instead, create a subfolder for exceptions, for easier management.

Many server administrators limit ownership to the Administrators as a group, except for a few situations. The folders typically owned by users include subfolders within their home folders and subfolders within publicly shared folders. Users can create and own subfolders within a folder where they have appropriate permissions.

## Configuring Permissions

Use the Add and Remove buttons on the folder properties Security tab to change which groups and users have permissions for a folder. To add a group, for example, click Add, scroll to the group you want to add, double-click that group, click OK, and then select the permissions. Also, for groups and users that are already set up with permissions, you can modify the permissions by clicking the group and checking or removing checks in the Allow and Deny columns, as shown in Figure 9-10. However, if *Allow inheritable permissions from parent to propagate to object* is checked, then selected Allow and Deny boxes are shaded and cannot be changed until this option is unchecked. **Inherited permissions** are similar to inherited rights in that the same permissions on a parent object, such as a folder (or the root), apply to child objects, such as files and subfolders within the parent folder. Allowing permissions to propagate from the parent object means that the permissions used by a higher-level folder are inherited by the child objects that have this box checked. To remove the propagation of inheritable permissions, remove the check in the box and click Remove in the Security dialog box (see Figure 9-11); or, to set up permissions that are inherited from the parent, place a check in the box and click Copy.

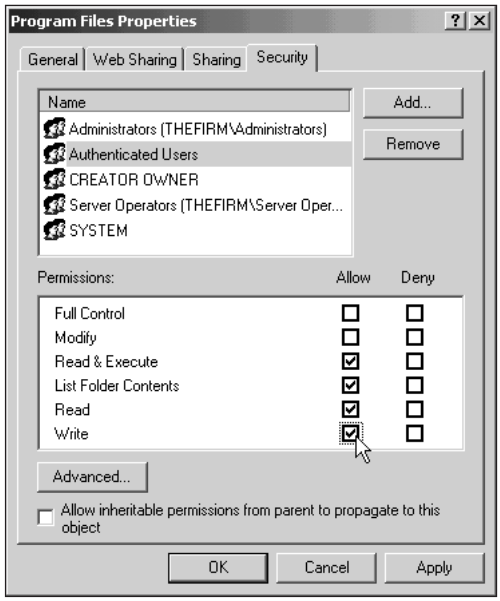



**Figure 9-10** Configuring permissions by groups and users

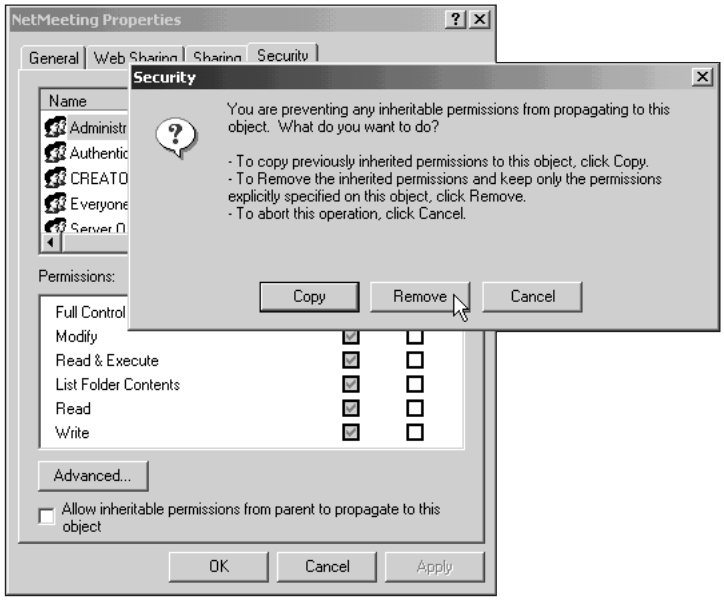



**Figure 9-11** Configuring inherited permissions

Table 9-6 lists the folder and file permissions supported by NTFS.

**Table 9-6** NTFS Folder and File Permissions

| Permission | Description | Applies to |
|---|---|---|
| Full Control | Can read, add, delete, execute, and modify files plus change permissions and attributes, and take ownership | Folders and files |
| List Folder Contents | Can list (traverse) files in the folder or switch to a subfolder, view folder attributes and permissions, and execute files, but cannot view file contents | Folders only |
| Modify | Can read, add, delete, execute, and modify files, but cannot delete subfolders and their file contents, change permissions, or take ownership | Folders and files |
| Read | Can view file contents and view folder attributes and permissions, but cannot traverse folders or execute files | Folders and files |
| Read & Execute | Implies the capabilities of both List Folder Contents and Read (traverse folders, view file contents, view attributes and permissions, and execute files) | Folders and files |
| Write | Can create files, write data to files, appended data to files, create folders, delete files (but not subfolders and their files), and modify folder and file attributes | Folders and files |


If none of the Allow or Deny boxes is checked, then the associated group or user has no access to the folder (with the exception of a selected user who has access via a group). Also, when a new folder or file is created, it typically inherits permissions from the parent folder or from the root.

If you need to customize permissions, you have the option to set up special permissions for a particular group or user. For example, consider a situation in which you want to give a user account the equivalent of Full Control permissions, but without the ability to take ownership (leaving that permission to administrators only):

1. Open the folder properties dialog box by right-clicking the folder and clicking Properties.
2. Click the Security tab.
3. Click the user account in the Name text box or click Add, scroll to find the user account in the Select Users, Computers, or Groups dialog box, and double-click the account. Click OK.
4. Click the user account after adding it, and then click the Allow box for Full Control.
5. Click the Advanced button.
6. Scroll to and click the user account under the Permission Entries box, if the account is not already selected.

7. Click the View/Edit button.
8. Scroll to the bottom of the list of special permissions (see Figure 9-12) to find Take Ownership, and check the Deny box. Click OK.
9. Click OK. Click Yes if you see a warning box about using the Deny entry. Click OK again to leave the Properties dialog box.

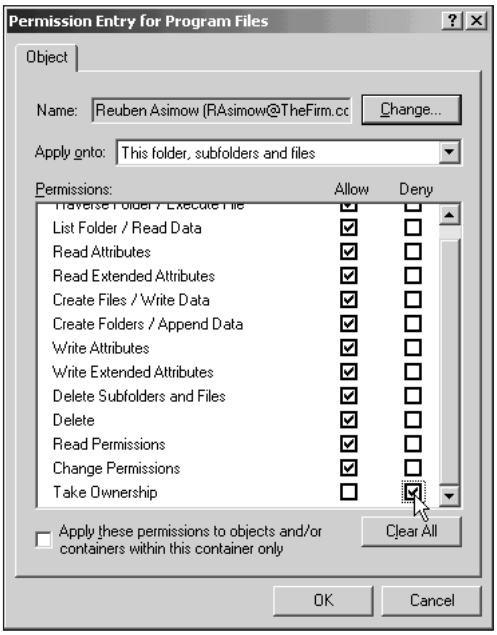



**Figure 9-12** Configuring special permissions

The option at the bottom of the dialog box, *Apply these permissions to objects and/or containers within this container only*, enables you to designate that the special permissions apply to the current folder and its files only, and are not inherited by subfolders. You can fine-tune inheritance by using options in the *Apply onto* list box, which include applying the permissions strictly to:

- This folder only
- This folder, subfolders, and files
- This folder and subfolders
- This folder and files
- Subfolders and files only
- Subfolders only
- Files only

Table 9-7 summarizes the special permissions. Hands-on Project 9-6 enables you to practice setting up permissions and special permissions.

**Table 9-7** NTFS Folder and File Special Permissions

| Permission | Description | Applies to |
|---|---|---|
| Traverse Folder/ Execute File | Can list the contents of a folder and execute program files in that folder; keep in mind that all users are automatically granted this permission via the Everyone and Users groups, unless it is removed or denied by you | Folders (Traverse Folder)<br>Files (Execute File) |
| List Folder/ Read Data | Can list the contents of folders and subfolders and read the contents of files | Folders (List Folder)<br>Files (Read Data) |
| Read Attributes | Can view folder and file attributes (Read-only and Hidden) | Folders and files |
| Read Extended Attributes | Enables the viewing of extended attributes (Archive, Index, Compress, Encrypt) | Folders and files |
| Create Files/ Write Data | Can add new files to a folder and modify, append to, or write over file contents | Folders (Create Files)<br>Files (Write Data) |
| Create Folders/ Append Data | Can add new folders and add new data at the end of files (but not delete, write over, or modify data) | Folders (Create Folders)<br>Files (Append Data) |
| Write Attributes | Can add or remove the Read-only and Hidden attributes | Folders and files |
| Write Extended Attributes | Can add or remove the Archive, Index, Compress, and Encrypt attributes | Folders and files |
| Delete Subfolders and Files | Can delete subfolders and files (the following Delete permission is not required) | Folders and files |
| Delete | Can delete the specific subfolder or file to which this permission is attached | Folders and files |
| Read Permissions | Can view the permissions (ACL information) associated with a folder or file (but does not imply that you can change them) | Folders and files |
| Change Permissions | Can change the permissions associated with a folder or file | Folders and files |
| Take Ownership | Can take ownership of the folder or file (Read Permissions and Change Permissions automatically accompany this permission) | Folders and files |

Microsoft provides guidelines for setting permissions, as follows:

- Protect the Winnt folder that contains operating system files on Windows 2000 servers and workstations, and its subfolders, from general users by allowing limited access, such as Read & Execute and List Folder Contents, or by just using the special permission to Traverse Folder/Execute File, but give the Administrators group Full Control access
- Protect server utility folders, such as those for backup software and network management, with access permissions only for Administrators, Server Operators, and Backup Operators

- Protect software application folders with Read & Execute and Write to enable users to run applications and write temporary files
- Create publicly used folders to have Modify access, so users have broad access except to take ownership, set permissions, and delete subfolders and their contents
- Provide users Full Control of their own home folders
- Remove the groups Everyone and Users from confidential folders, such as those used for personal mail, for sensitive files, or for software development projects


Always err on the side of too much security. It is easier, in terms of human relations, to give users more permissions later than it is to take away permissions.

## Configuring Auditing



Accessing folders and files can be tracked by setting up auditing. Some organizations choose to implement auditing on folders and files that involve financially sensitive information, such as those involving accounting and payroll. Other organizations monitor access to research or special marketing project information stored in folders and files. Windows 2000 Server NTFS folders and files enable you to audit a combination of any or all of the activities listed as special permissions in Table 9-7. When you set up auditing, the options for each type of access are to track successful and failed attempts, as shown in Figure 9-13. For example, consider a situation in which your organization's financial auditors specify that all accounting files in the Accounting folder must create an "audit trail" for each time a person who has access changes the contents of a file in the folder. Further, the only groups that have access to write to files are those in the Accounting and Administrator groups. You would set up auditing by configuring the folder's security to audit each successful type of write event, such as Create Files/Write Data and Create Folders/Append Data. For extra information, you might track permission, attribute, and ownership changes by monitoring successful attempts to Write Attributes, Write Extended Attributes, Change Permissions, and Take Ownership. Audited events are recorded in the Windows 2000 Security log that is accessed from the Event Viewer (see Chapter 16).

You can set up folder auditing through these steps:

1. Right-click the folder you want to audit, and click Properties.
2. Click the Security tab.
3. Click the Advanced button.
4. Click the Auditing tab in the Access Control Settings dialog box, and click Add.
5. Double-click the group you want to audit.
6. Check the Successful or Failed events that you want to audit, and click OK.
7. Click OK and click OK again to exit the Access Control Settings and the Properties dialog boxes.

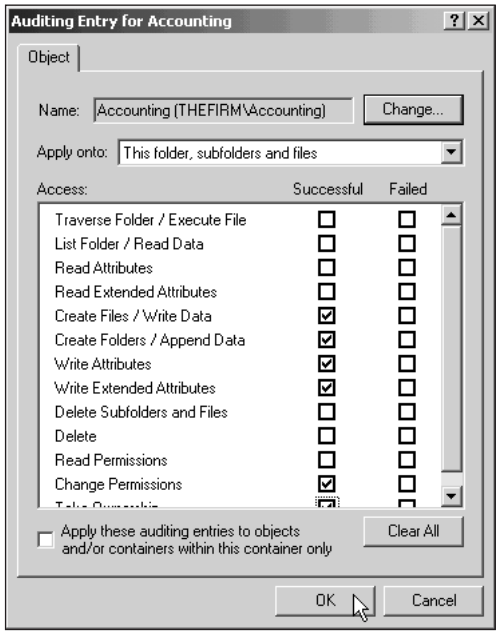



**Figure 9-13** Configuring folder auditing

## Troubleshooting Auditing

You cannot configure auditing for an object—an account or folder, for example—unless an auditing policy is already set up. If the policy is not set up, you will see an error message at Step 7, stating that the folder auditing cannot be configured. To configure an auditing policy that enables you to audit folder activity, start by modifying the group policy on a standalone server or the default domain policy on a server governed by the Active Directory. For example, you modify the default domain policy by using the following steps:

1. Open the Active Directory Users and Computers tool, and right-click the domain in which you want to modify the policy.
2. Click Properties and click the Group Policy tab.
3. Click Default Domain Policy and click Edit.
4. As necessary to expand the view in the tree, double-click Windows Settings under Computer Configuration, double-click Security Settings, and double-click Local Policies.
5. Double-click Audit Policy to view its options.
6. Double-click Audit object access.
7. Check Define these policy settings in the template, check Success, and check Failure. Click OK (see Figure 9-14).

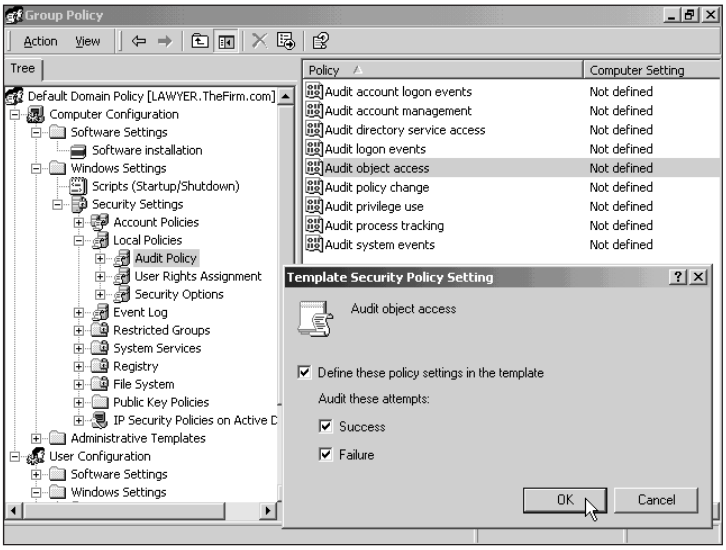



**Figure 9-14** Configuring audit policy as part of the default domain policy

9

Also, if you are logged on but cannot configure auditing or view audited events in the Event viewer, check to make sure that you are logged on using an account that is a member of the Domain Admins group. Audit information is stored in the *system control access list,* which is a special security descriptor (list) that is associated with objects when auditing is turned on. Domain Admins have privileges to set up and modify the system control access list.

## Configuring Ownership

With permissions and auditing set up, you may want to verify the ownership of a folder. Folders are first owned by the account that creates them, for example the Administrator account. Folder owners have the ability to change permissions for the folders they create. Also, ownership can be transferred only by having the Take Ownership special permission or Full Control Permission (which includes Take Ownership). These permissions enable a user to take control of a folder or file and become its owner. Taking ownership is the only way to shift control from one account to another. The Administrators group always has the ability to take control of any folder, regardless of the permissions, particularly because there are instances in which the server administrator needs to take ownership of a folder, such as when someone leaves an organization.

To take ownership of a folder, right-click the folder, click Properties, click the Security tab, click the Advanced button, and click the Owner tab. Select the account or group that will take ownership, such as the Administrators group, and click OK. Click OK again to exit the Properties dialog box.

## Configuring Share Permissions to Share a Folder on the Network

Along with establishing permissions, auditing, and ownership, a folder can be set up as a shared folder for users to access over the network. To share a server folder, access the Sharing tab in the folder properties dialog box (right-click the folder and click Sharing). As Figure 9-15 shows, the Sharing tab has two main options: to share or to not share the folder. To share a folder so network users can access or map it, click the Share this folder button. Figure 9-15 shows the folder Public shared with the share name Public, for general sharing. The Maximum allowed button enables as many accesses as there are Windows 2000 Server client access licenses. The other option, Allow ____ Users, enables you to specify a limit to the number of simultaneous users. This is one way to ensure that the licensing restrictions for software are followed.

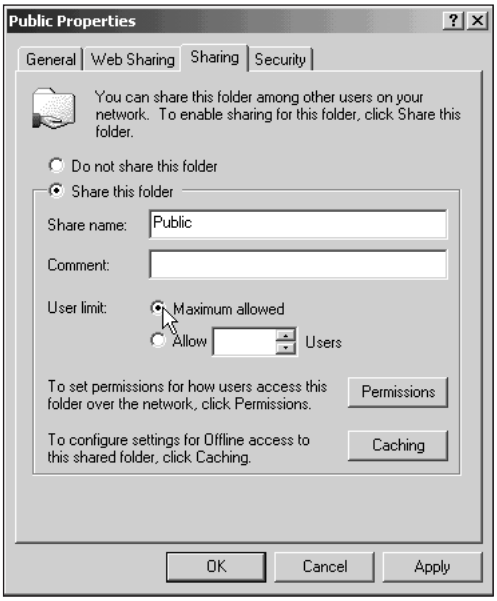



**Figure 9-15** Configuring a shared folder

For example, suppose that you have an accounting software package in a folder and have only two licenses. In this case you would set the Allow ____ Users parameter to 2 so the license requirement is honored.

You can set permissions for the share from this tab by clicking the Permissions button. As explained earlier, share permissions for an object can differ from basic access permissions set through the Security tab, and the permissions are cumulative, with the exception of permissions that are denied. There are three share permissions that are associated with a folder:

- *Read:* Permits groups or users to read and execute files
- *Change:* Enables users to read, add, modify, execute, and delete files
- *Full Control:* Provides full access to the folder, including the ability to take control or change permissions

Before setting the share permissions, make sure you have selected the appropriate groups and users, for example by specifying the Everyone or Users groups for a publicly accessed folder. Use the Add button in the Permissions dialog box to set up additional groups, and the Remove button to delete a group's access to a shared folder. For example, you can remove a group by highlighting it in the list box in the Access Through Share Permissions dialog box and clicking Remove. To set the share permissions, highlight a group, and click the appropriate Allow and Deny boxes for the permissions.

The Caching button in Figure 9-15 enables you to set up a folder so that it can be accessed by a client even when the client computer is not connected to the network, for instance when the network connection is lost or when a user disconnects a laptop computer to take it home. Caching in this situation means that the folder is cached on the client computer's hard drive for continued access after losing the network connection, and that the folder location remains unchanged in Windows Explorer and My Computer. When the network connection is resumed, any cached files that have been modified can be synchronized with the network versions of the files. If two or more users attempt to synchronize a file, they have the option of choosing whose version to use or of saving both versions. A folder can be cached in three ways:



- *Automatic Caching for Documents:* Documents are cached without user intervention, which means that all files in the folder that are opened by the client are cached automatically.
- *Manual Caching for Documents:* Documents are cached only per the user's request per each document (the default option).
- *Automatic Caching of Programs:* Document and program files are automatically cached when opened, but their contents cannot be modified (which means that you must also set the shared folder permissions to Read).


There is an option to hide a shared folder so that it does not appear on a browser list—in My Network Places in Windows 2000 or Network Neighborhood in Windows 98 or Windows NT, for example. To hide a share, place the $ sign just after its name. For instance, if the Share name text box contains the share name Budget, you can hide the share by entering Budget$. (This is an actual example of what one university does to discourage general scanning of a folder containing budget worksheets. However, department accounting technicians who know of the folder's existence can map it to help with budget planning.)


When you right-click on a folder to view its properties, the sharing option on the shortcut menu may be missing, or you may not see the Sharing tab. You can troubleshoot this problem by making sure that the Server service is started, and even if it is, you can restart it in case the service is hung (make sure no users are logged on if you restart it). To start or restart the Server service, click Start, point to Programs, point to Administrative Tools, and click Computer Management. Double-click Services and Applications, double-click Services, scroll to the Server service, and check for "Started" in the status column. Right-click the service; if it is stopped, click Start, and if it is already started, click Restart. After clicking Restart, a dialog box is displayed showing that other services will restart as well. Click Yes to restart the services.

To help guide you through the steps of creating a shared folder, Windows 2000 Server also offers the Shared Folder Wizard. To open the wizard, click the Start button, point to Programs, point to Administrative Tools, and click Configure Your Server. Next, click File Server on the menu in the left side of the screen and click the Start hyperlink to start the wizard. Try Hands-on Project 9-7 to set up a shared folder.

## Web Sharing

Some folders and files stored in Windows 2000 Server may be intended for HTML or FTP access through a Web server (see Chapters 3 and 13). The Web server can be the same or a different Windows 2000 server from the one on which the folders and files reside. Use the following steps to set up a folder for Web sharing and to configure its Web sharing permissions:

1. Right-click the folder, click Properties, and click the Web Sharing tab.
2. Use the *Share on* box to specify the Default Web site or Administration Web Site on which the folder will be shared.
3. Click Share this folder.
4. Specify an alias for the folder, which enables clients to view it by a name other than the actual folder's name.
5. Check the appropriate access permissions from among the selections: Read, Write, Script source access, and Directory browsing (see Figure 9-16).

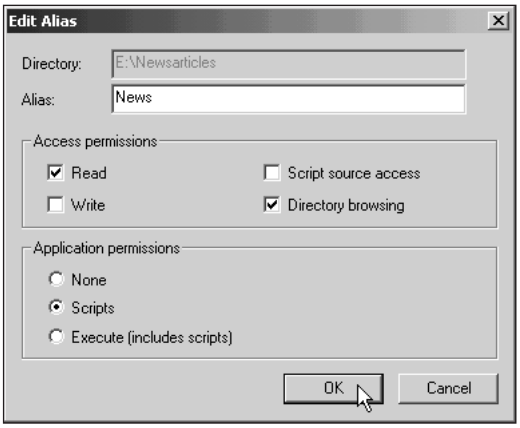



**Figure 9-16** Entering Web sharing permissions

6. Check the application permissions from among the selections: None, Scripts, and Execute (includes scripts).
7. Click OK and click OK again to save your changes.

Tables 9-8 and 9-9 show the Web sharing application permissions and access permissions.

**Table 9-8** Web Sharing Access Permissions

| Access Permission | Description |
|---|---|
| Read | Enables clients to read and display the contents of folders and files via the Internet or an intranet |
| Write | Enables clients to modify the contents of folders and files; includes the ability to upload files through FTP |
| Script source access | Enables clients to view the contents of scripts containing commands to execute Web functions |
| Directory browsing | Enables clients to browse the folder and subfolders, for example for FTP access |

**Table 9-9** Web Sharing Application Permissions

| Application Permission | Description |
|---|---|
| None | No access to execute a script or application |
| Scripts | Enables the client to run scripts to perform Web-based functions |
| Execute (includes scripts) | Enables clients to execute programs and scripts via the Internet or an intranet connection |

## Troubleshooting a Security Conflict

Sometimes you will set up access for a user, but find that the user does not actually have the type of access you set up. Consider the example of Cleo Jackson, an English professor who maintains a shared subfolder called Assignments for his students from the account CJackson. Assignments is a subfolder under the parent folder English, which contains folders used by all English professors. CJackson needs to update files, copy in new files, and delete files. As Administrator, you have granted CJackson Modify access permissions to Assignments. However, you omitted the step of reviewing the groups to which CJackson belongs, such as the Paper group, which consists of Cleo Jackson and the student newspaper staff. The Paper group has been denied all access to the English folder and all of its subfolders. When Cleo Jackson attempts to copy a file to the Assignments folder, he receives an access denied message.

To troubleshoot the problem, you should review the folder permissions and share permissions for the CJackson account and for all of the groups to which CJackson belongs. In this case, because the Paper group is denied access, CJackson is also denied. The easiest solution is to remove CJackson from the Paper group and perhaps create a group of English professors, such as EngProfs, who all have access to the same resources as the Paper group.

This example also illustrates how you save both time and user aggravation when you carefully plan in advance the folder and group structures in light of the network and server security needs.

## Moving and Copying Files and Folders

A common task is to move or copy files from one folder to another in the same volume or to a different volume. When a file is copied, the original file remains intact, and a copy is made in another folder. Moving a file causes it to be deleted from the original location and placed in a different folder on the same or on a different volume. Copying and moving work the same for a folder, but the entire folder contents (files and subfolders) is copied or moved. When a file or folder is created, copied, or moved, the file and folder permissions can be affected in the following ways (depending on how inheritance is set up in the target location):

- A newly created file inherits the permissions already set up in a folder.
- A file that is copied from one folder to another on the same volume inherits the permissions of the folder to which it is copied.
- A file or folder that is moved from one folder to another on the same volume takes with it the permissions it had in the original folder. For example, if the original folder had Read permissions for the Users domain local group and the folder to which it is transplanted has Modify permissions for Users, that file (or folder) will still only have Read permissions.
- A file or folder that is moved or copied to a folder on a different volume inherits the permissions of the folder to which it is moved or copied.

- A file or folder that is moved or copied from an NTFS volume to a folder in a FAT volume is not protected by NTFS permissions, but it does inherit share permissions if they are assigned to the FAT folder.
- A file or folder that is moved or copied from a FAT volume to a folder in an NTFS volume inherits the permissions already assigned in the NTFS folder.

Windows 2000 Server offers many ways to move and copy files and folders. You can use the right-click or left-click drag methods. Right-click the file or folder you want to copy or move, and while holding down the right mouse button, drag it into the folder to which you want it copied or moved. When you release the right mouse button, click Copy Here or Move Here on the shortcut menu. If you use the left mouse button to click and drag a file or folder, it moves or copies without presenting the shortcut menu. When you use the left mouse button, the file or folder is moved if the destination is on the same volume or disk; it is copied if the destination is on a different volume or disk. Another way to move and copy files and folders is to use the Cut, Copy, and Paste options in the Edit menu of My Computer and Windows Explorer.


If you discover you have moved or copied the wrong file or folder, immediately click the Undo button on the button bar in My Computer or Windows Explorer.



## Chapter Summary

- Windows 2000 Server groups offer a particularly effective way to manage user accounts and server resources such as access to specific servers, folders, and files. A Windows 2000 server that is used as a standalone computer has one type of management security group called a local group. When the Active Directory is implemented, three kinds of security groups exist: domain local, global, and universal. Your advance planning in terms of how to set up and use groups will be one of the most effective tools to save you time as administrator and to provide thorough security for your network.
- As you learned in Chapter 4, Windows 2000 Server objects are managed through an access control list that provides information about which user accounts and groups can access an object, such as a folder or file. There are many ways to control access, including user rights, inherited permissions, permissions, share permissions, Web permissions, auditing, and ownership. Managing access is a potentially complex process that is made easier by managing through groups and group membership rather than by managing individual accounts.
- Even when you manage access through groups, conflicts can occur that result in some users having too little access and other users having too much. One rule to use when you troubleshoot an access problem is to review the types of groups used and the group memberships, and to particularly look for situations in which a user belongs to one group that has access and another that is denied access. Also, as you create, copy, and move folders and files, make sure that you understand how access is inherited.

In the next chapter, you learn more about managing access to folders and files by setting up the Distributed File System. Also, you learn how to install and manage disk quotas and application software.

## KEY TERMS

**attribute** — A characteristic associated with a folder or file used to help manage access and backups.

**auditing** — Tracking the success or failure of events associated with an object, such as writing to a file, and recording the audited events in an event log of a Windows 2000 server or workstation.

**domain local security group** — A group that is used to manage resources—shared folders and printers, for example—in its home domain, and that is primarily used to give global groups access to those resources.

**Encrypting File System** (**EFS**) — Set by an attribute of NTFS, this file system enables a user to encrypt the contents of a folder or a file so that it can only be accessed via private key code by the user who encrypted it. EFS adheres to the Data Encryption Standard's expanded version for data protection.

**global security group** — A group that typically contains user accounts from its home domain, and that is a member of domain local groups in the same or other domains, so as to give that global group's member accounts access to the resources defined to the domain local groups.

**inherited permissions** — Permissions of a parent object that also apply to child objects of the parent, for example to subfolders within a folder.

**inherited rights** — User rights that are assigned to a group and that automatically apply to all members of that group.

**local security group** — A group of user accounts that is used to manage resources on a standalone Windows 2000 server that is not part of a domain.

**mixed mode** — An Active Directory context in which there are both Windows NT 4.0 domain controllers (PDC and BDCs) and Windows 2000 Server domain controllers (DCs).

**native mode** — An Active Directory context in which there are only Windows 2000 Server domain controllers (DCs).

**ownership** — Having the privilege to change permissions and to fully manipulate an object. The account that creates an object, such as a folder or printer, initially has ownership.

**permissions** — In Windows 2000, privileges to access and manipulate resource objects, such as folders and printers; for example, privilege to read a file, or to create a new file.

**scope of influence** — The reach of a type of group, such as access to resources in a single domain or access to all resources in all domains in a forest (see domain local, global, and universal groups). (Another meaning for the term *scope* is the beginning through ending IP addresses defined in a DHCP server for use by DHCP clients; see Chapter 13.)

**share permissions** — Special permissions that apply to a particular shared object, such as a shared folder or printer.

**universal security group** — A group that is used to provide access to resources in any domain within a forest. A common implementation is to make global groups that contain accounts members of a universal group that has access to resources.

## Review Questions

1. Your college's president has several sensitive budget spreadsheets located in the Budgets subfolder under her home folder on a Windows 2000 server, and she wants to make sure that only she can read them. How can she set up security to be sure that only she can access and read those files?
   a. Use the Encrypting File System to protect the files in her Budgets subfolder.
   b. Set up the Users and Everyone groups to be denied access to the Budgets subfolder via all permissions.
   c. Set up the president's account password so it must be changed every week.
   d. Hide the Budgets subfolder by using the "$" character at the end.
2. You have set up a special Planning folder for the Promotions Planning Task force composed of members of the Marketing Department at your corporation. The folder is set up to give the Promo domain local group Full Control access permissions and Full Control share permissions. Also, you have a global group, called GlobalPromo, that contains only the members of the task force and is a member of the Promo group. However, after you set up the folder, no one in the GlobalPromo group can access it. Which of the following might explain why?
   a. You set up the Promo group to have Full Control access to the Planning folder, but denied ownership permission.
   b. You failed to set up automatic document caching for the Planning folder for the GlobalPromo group.
   c. You earlier made the GlobalMkt group a member of the Promo group, but also denied all permission access for GlobalMkt to the Planning folder when you set up the folder.
   d. all of the above
   e. only a and b
   f. only a and c
3. Last week you set up the AR folder for the Accounting Department as a shared folder and had members of that department successfully test their access to it. This morning several members of the Accounting Department report that they cannot access the folder. Also, one of your assistants is calling to report that he cannot set up a new shared folder on the server because there is no Sharing tab. What might be the problem?
   a. The Sharing service did not start properly on the server.
   b. The Server service did not start properly on the server.
   c. The Domain Local Policy Manager detected a sharing violation and turned off sharing.
   d. all of the above
   e. only a and b
   f. only b and c

4. You have an Active Directory structure that contains four domains. How might you plan to use groups in this situation?
   a. Use global groups to provide access to resources and domain local groups to contain user account members.
   b. Use only local groups to manage all access because you do not have enough domains to merit using universal groups.
   c. Use domain local groups and universal groups to manage resources and global groups to contain user account members.
   d. Use only universal groups because they are the best management technique when you have more than two domains.
5. Which of the following is not a Web sharing application permission?
   a. None
   b. Full Control
   c. Scripts
   d. Execute
6. You want to set up auditing on a sensitive folder. From where do you set it up?
   a. the Properties dialog box for that folder, using the Sharing tab
   b. the Control Panel, using the System icon
   c. the Active Directory Domains and Trusts tool
   d. the Properties dialog box for that folder, using the Security tab
7. When you attempt to set up auditing on a folder, you receive an error message indicating that you cannot set it up. What might be the cause of the problem?
   a. You have not enabled auditing an object as a group policy.
   b. The auditing service is not set to start automatically.
   c. You do not have the Active Directory installed.
   d. You are trying to set up auditing on a folder that is formatted for NTFS instead of FAT.
8. The CEO of your company is very angry because he lost important data while developing a critical spreadsheet for his board of directors meeting. He lost the data because his network connection was inadvertently cut by the construction firm hired to rewire parts of the network. How can you solve this problem so that it does not cause loss of data again?
   a. Hire a more careful construction company next time.
   b. Purchase a UPS for the CEO's computer.
   c. Set up certain folders, such as those used by the CEO, for caching.
   d. Use the folder Backup tool to automatically replicate certain folders at short intervals.

9. One way to reflect the organizational unit (OU) structure in a domain for security purposes is to
   a. create a universal group containing all members of all OUs.
   b. nest global groups to reflect the OU structure.
   c. use global groups to manage resources instead of domain local groups.
   d. make a local group for each OU's account composition.
10. You are making the first universal group, but find that the universal group option is deactivated. What is the problem?
    a. You must first install the Universal Grouping Service component in Windows 2000 Server.
    b. You have not first created any domain local groups.
    c. Universal groups can only hold user account members, and you are trying to use a domain local group as a member.
    d. You are running in mixed mode and must convert to native mode.
11. Martha was the accountant for your small company, but has now left, and you disabled her account. Unfortunately, her home folder on the server contains several vital accounting spreadsheets that one of the managing partners needs, but no one can access her home folder, including you as administrator. What is the best way to provide access to the information so that key company members can get to it?
    a. Enable the account, change the password, and give the password only to those who need it.
    b. Take ownership of Martha's home folder, change the permissions, and set up a share for those who need the information.
    c. Rename Martha's home folder, back it up, copy it into a publicly accessed shared folder, and hide that folder.
    d. Contact Martha to come back for a short time and distribute her data to those who need it.
12. With which of the following caching options should you set share permissions to Read?
    a. automatic caching of programs
    b. automatic caching for documents
    c. manual caching for documents
    d. none of the above because all must be set for Full Control access
13. One of the limitations of universal groups is that
    a. they cannot span domains.
    b. they cannot have global groups as members.
    c. they can only be used as distribution groups and not as security groups.
    d. none of the above is true.
    e. all of the above are true.

14. Which of the following are default global groups?
    a. Domain Guests
    b. Enterprise Admins
    c. Everyone
    d. all of the above
    e. only a and b
    f. only a and c
15. As administrator, you have set up a shared folder for the Inventory Department manager, and you ask him to take ownership and set up the permissions he wants. Later you receive a telephone call from him about a problem with a file in that folder. You log on to your account, which is a member of Domain Admins, and find that you cannot access the shared folder. Why not? (After all, you created it.)
    a. Even administrators cannot access files owned by another user.
    b. The problem with the file has spread to the entire folder, and the folder must be restored.
    c. The Inventory Department manager did not set up permissions access for the Builtin Administrators group or for Domain Admins.
    d. You must have ownership to access a folder through Domain Admins.
16. You are consulting for a doctor's office consisting of 18 networked workstations and one Windows 2000 server that is used to share folders. The office has a demo of a new medical database, but the licensing requires that not more than two people access it at the same time. How can you accommodate this requirement most easily?
    a. Set up the database in a hidden folder, because the access limit on a hidden folder is 2.
    b. Set up the database in a shared folder and set the user limit to 2.
    c. Set up the database in a shared folder, but change the permissions daily to a different combination of two people.
    d. Set up user rights to the server so that no more than two people can access the server at once.
17. The director of finance has called you into a planning meeting because your school has just determined that an accountant who quit four months ago embezzled $50,000 from the school. Besides setting permissions, the director wants to know other ways to help prevent this type of situation. What do you recommend?
    a. Deny access to log on locally to Windows 2000 servers.
    b. Establish an alert to the Administrators group whenever specific folders and files are accessed.
    c. Set up auditing on specific folders and files and regularly review the audit reports.
    d. Regularly remove the Archive attribute on specific folders so you can track how often they are accessed.

18. When you copy a file from a disk in drive A into an NTFS-formatted folder, what permissions are associated with the new file in the NTFS folder?
    a. The new file will not have any permissions set up.
    b. The new file will inherit the permissions set up for the NTFS folder.
    c. The new file can only be accessed by you, until you set up permissions.
    d. The new file will give the Users group Read permissions by default.
19. Access to Debug programs is an example of
    a. a special permission.
    b. an access permission.
    c. an attribute.
    d. a user right.
20. Which of the following are examples of extended attributes, and in which file system?
    a. Read only and Hidden in FAT
    b. Read only and Hidden in NTFS
    c. Archive and Compress in FAT
    d. Archive and Compress in NTFS
21. Yesterday your assistant was working with permissions and user rights, and today the Research group cannot access anything on your organization's Windows 2000 server. What might be the problem?
    a. He took away the permission for that group to access the TCP/IP driver.
    b. He removed or denied the user right for that group to access the server from the network.
    c. He removed ownership access to the \Public folder for the group.
    d. He changed the Full Control permissions to Read and Write on the shared drives the group accesses.
22. You have converted from mixed mode to native mode, but now want to convert back. How can you do that?
    a. Convert the mode in the Default Domain Policies.
    b. Convert using the Active Directory Domains and Trusts tool.
    c. Convert using the Active Directory Users and Computers tool.
    d. There is no tool that will enable you to convert back.
23. Which type of access control enables you to compress the contents of a folder?
    a. a permission
    b. a special permission
    c. a user right
    d. an attribute
    e. an auditing parameter

24. Your boss is a busy person and wants you to give him ownership of several folders so that he does not have to spend time on the task. As administrator, how do you accomplish transferring ownership?
    a. Simply give him Take Ownership permission, and he has ownership.
    b. Give him Full Control permissions and then transfer ownership to him.
    c. You can give him Take Ownership permission, but he must take ownership himself.
    d. Add him to the Domain Administrators group, and he automatically has ownership.
25. The Math Department head needs two files that you have in your folder, access to which is denied to anyone but you. What type of access will he have to the files after you simply move them to his folder?
    a. no access
    b. the access inherited from his folder
    c. ownership, but he must set his own permissions
    d. the Modify permissions

## HANDS-ON PROJECTS


### Project 9-1

This project gives you practice changing the mode (mixed to native) of a domain. You will need access to a domain controller and an account that has Administrator access for the domain. Also, check with your instructor about which domain to work on, and make absolutely sure you have permission to change modes before proceeding to Step 6 (otherwise you will simply view where to change modes).

**To change the mode of a domain:**

1. Start the MMC and make sure that the Active Directory Domains and Trusts snap-in is installed. If it is not, install it now.
2. Double-click **Active Directory Domains and Trusts**, and right-click the domain you want to work on.
3. Click **Properties**.
4. Make sure the General tab is displayed, and review its contents. Notice what other tabs are available, and click each one to briefly view its contents. Record your observations in a lab journal or in a word-processed document. Go back to the General tab.
5. What mode is currently set up? Is there a Change Mode button displayed on the tab? If it is not displayed, why not? If you have permission from your instructor to change modes and if the Change Mode button is displayed, go on to the next step. If not, click Cancel and close the MMC. Click No if you are asked to save the console settings.
6. Click the **Change Mode** button and click **Yes**.
7. Click **Apply** and notice the warning message that you must reboot for the change to take effect. Click **OK** to close the warning message.

8. Click **OK**, close the MMC, click **Yes** if asked to save your console settings, and shut down the domain controller (make sure no one is connected). Reboot.
9. Record and underscore an observation that you must reboot after changing modes, so you will have this information in the future.


## Project 9-2

In this project, assume that you have been asked to set up groups to manage access for the managers in an Active Directory that has four domains. You will practice beginning the setup by creating a domain local group that will be used to manage resources and a global group of accounts. Last, you will add the global group to the domain local group. To complete the assignment, you will first need an environment in which the Active Directory is installed and two accounts that are already set up by your instructor. If your instructor asks you to set up your own accounts for practice, refer to Chapter 8 and create two accounts in which the usernames are built from your first initial, last name, and a unique number at the end, for example RBrown1 and RBrown2.

**To set up the domain local group:**

1. Install and use the **Active Directory Users and Computers** snap-in in the MMC, or click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. Double-click **Active Directory Users and Computers** in the tree, and click a domain, such as **TheFirm.com**.
3. Double-click **Users**. Notice what default groups are already created under Users, and record these in your lab journal or in a word-processed document.
4. Click the **Action** menu, point to **New**, and click **Group**. What defaults are already selected in the New Object – Group dialog box? Record your observations.
5. In the Group name box, enter **DomainMgrs** plus your initials, for example **DomainMgrsMJP**. What is the pre-Windows-2000 group name?
6. Click **Domain local** under Group scope, and click **Security** (if it is not already selected) under Group type.
7. Click **OK** and then look for the group you just created in the right pane within the Users container.

**To create the global group and add it as a member of the local group:**

1. Make sure that the Users container is still open.
2. Click the **Create a new group in the current container** icon on the button bar.
3. In the Group name box, enter **GlobalMgrs** plus your initials, for example **GlobalMgrsMJP**.
4. Click **Global** under Group scope, and click **Security** under Group type, if they are not already selected.
5. Click **OK** and then look for the group you just created in the right pane. Double-click the global group you created.

6. Click the **Members** tab. Are there any members already associated with the group?
7. Click the **Add** button. Scroll through the choices of members. Can you add only user accounts or are there other choices? Can you add the DomainMgrs*XXX* group that you created? Record your observations.
8. Scroll to find one of the accounts set up for this assignment, and double-click that account.
9. Scroll to find the second account set up for this assignment, and double-click it.
10. Make sure that both accounts are displayed in the bottom text box, and then click **OK**.
11. Click the **Members Of** tab and click **Add**.
12. Find the domain local group that you created, for example **DomainMgrsMJP**, and double-click it. This step adds the global group you created to the domain local group. Click **OK**.
13. Click **Apply** and click **OK** (or just OK to save your changes).
14. Double-click the domain local group, such as **DomainMgrsMJP**, and then click the **Members** tab. What members are shown? How would you remove a member and add another?
15. Click **Cancel**, but leave the Console display open.
16. Explain in your lab journal or in a word-processed document how to set up the necessary management groups in the other three domains. Also, note how you might perform the tasks in this assignment differently by using universal groups. Try the next assignment for ideas about using universal groups.


## Project 9-3

In this hands-on activity, you will convert a domain local group to a universal group. (You must be working in a native mode domain to complete all of these steps.)

**To convert the group:**

1. Make sure that the Console is still open from Project 9-2 and also that the Users container is open.
2. Double-click the domain local group that you created in Project 9-2, for example **DomainMgrsMJP**.
3. Notice if any of the group scope selections are deactivated. If so, record which ones in your lab journal or in a word-processed document.
4. Click **Universal** under Group scope.
5. Click **OK**.
6. Double-click the group that you just converted, such as **DomainMgrsMJP**, and then click the **Members** tab. Did converting the group change the members? Record your observations.
7. Leave the Console window open for the next project.


## Project 9-4

In this hands-on activity, you configure user rights in the default domain policy (group policy for the domain). You will set up the rights so that the domain local group that you converted to a universal group has access to the server over the network and to backup files and folders.

**To configure the user rights:**

1. Right-click the domain, such as **TheFirm.com**, in the Console tree under Active Directory Users and Computers.
2. Click **Properties** and then click the **Group Policy** tab.
3. If necessary, click **Default Domain Policy** under Group Policy Object Links, and click **Edit**.
4. As necessary to expand the view in the tree, double-click **Windows Settings** under Computer Configuration, double-click **Security Settings**, and double-click **Local Policies**.
5. Double-click **User Rights Assignment**. Notice the user rights that are available, and record some examples in your lab journal or in a word-processed document.
6. Double-click **Access this computer from the network** under the Policy column in the right pane.
7. Click **Define these policy settings** (if there is no check in the box), and then click **Add**.
8. Click the **Browse** button.
9. Find the domain local group that you made into a universal group in Hands-on Project 9-3, for example **DomainMgrsMJP**, and double-click it. Click **OK** in the Select users or Groups dialog box, click **OK** in the Add user or group dialog box, and click **OK** in the Security Policy Setting dialog box.
10. Under Policy in the right pane, double-click **Back up files and directories**.
11. Repeat Steps 7, 8, and 9.
12. How does the action you have just taken affect the users in the GlobalMgrs*XXX* group that you created in Hands-on Project 9-2?
13. Close the Group Policy window, and click **OK** in the domain properties dialog box.
14. Close the Active Directory Computers and Users console.


## Project 9-5

In this project, you practice encrypting the contents of a folder, which enables you to use the Encrypting File System (EFS).

**To encrypt a folder:**

1. Use My Computer or Windows Explorer to create a new folder. For example, open **My Computer** on the desktop, double-click a local drive (NTFS formatted), such as drive **C**, click **File**, point to **New**, click **Folder**, and enter a folder name that is a combination of your last name and initials, for example **RLBrown**, and press **Enter**. Find a file to copy into the folder, such as a text or another file already in the root of drive C. To copy the file, right-click it, drag it to the folder you created, and click **Copy Here**.

2. Right-click your new folder—**RLBrown**, for example—and click **Properties**. Make sure that the **General** tab is displayed, and if it is not, then click it.
3. What attributes are already checked? Record your observations.
4. Click the **Advanced** button. Record which attributes are already checked in the Advanced Attributes dialog box.
5. Check **Encrypt contents to secure data**, and then click **OK**.
6. Click **Apply**.
7. Click **Apply changes to this folder, subfolders and files**, and click **OK**.
8. Click **OK**.
9. Note in your lab journal or in a word-processed document how you would verify that the file you copied into the folder is now encrypted. How would you decrypt the entire folder contents?
10. Decrypt the folder and leave it so that you can use it for the next project.


## Project 9-6

In this project, you will practice setting up folder permissions and special permissions.

**To set up permissions and special permissions:**

1. Right-click the new folder you created in Project 9-5, click **Properties**, and then click the **Security** tab.
2. What users and groups already have permissions to access the folder, and what are the permissions?
3. Remove the check from **Allow inheritable permissions from parent to propagate to this object**, and click **Remove**. What access is available to the folder now?
4. Click **Add**.
5. Double-click **Users** and click **OK**. What permissions are automatically granted? Record your observations.
6. Click the **Allow** box for the **Write** permission.
7. Click the **Advanced** button. What options are available from the dialog box that is displayed?
8. Make sure that the **Users** group is highlighted in the Permissions Entries text box, or click Users if the group is not highlighted.
9. Click **View/Edit**. Notice and record the special permissions that are already set up.
10. Open the **Apply onto** list box and click **Subfolders and files** only.
11. Click the **Allow** box for the **Delete Subfolders and Files** special permission.
12. Click **OK**, and click **OK** again.
13. What permissions now show for the folder for the Users group? Why?
14. Use the **Add** button and give the Server Operators group Full Control.
15. Click **OK** to save your changes, and exit the Properties dialog box. Open the Properties dialog box again to check your work, and then close it.


## Project 9-7

This Hands-on Project gives you practice configuring the folder you created in Hands-on Project 9-5 as a shared folder.

**To configure the shared folder:**

1. Right-click the new folder you created in Project 9-5, and click **Sharing**.
2. Click the **Share this folder** button on the Share tab. What share name is entered automatically?
3. Enter **Test share** as the comment.
4. Click the **Allow Users** button and enter **20** as the maximum number of clients who can simultaneously access this folder.
5. Click **Permissions**. Record the groups and access permissions that are displayed by default.
6. Click the **Everyone** group, if it is displayed, and click **Remove**.
7. Click the **Add** button.
8. Double-click **Server Operators** and click **OK**. Record the resulting access permissions that are available for a shared folder and the permissions that are now selected by default.
9. Click the **Allow** box for **Full Control**, and record how the permissions change. Click **OK**.
10. Click the **Caching** button, click **Allow caching of files in this shared folder** (if it is not already checked), and select **Automatic Caching for Documents** in the Setting box. Click **OK**.
11. Click **OK** to save your changes to the folder's properties and ACL.
12. Delete the folder you created by right-clicking it, clicking **Delete**, and clicking **Yes**. Click **Yes** again to the warning that others may be using files in the folder. Close My Computer or Windows Explorer.



# CASE PROJECT


## Aspen Consulting Project: Configuring Folder Management and Security

Mark Arnez has assigned you to work with a large restaurant called Feasters that specializes in serving giant meals. Feasters has a small network of 15 client workstations and one Windows 2000 server. Seven of the workstations are stationed throughout the restaurant and are used by the table servers to place customer orders. Five workstations are used by the owner and the business management staff, and three workstations are in the kitchen for the chef's staff. Feasters has hired you to set up the Windows 2000 server and to train two of the business management staff on its operation.

1. Feasters is at one location now, but they are negotiating to purchase four more restaurants to turn into new Feasters within one year. All of the new restaurants will be networked

into the main Windows 2000 server you are setting up at the first location. Explain how you would work with the current management staff to determine how to set up groups now that will enable them to be ready for the future. What natural groupings can you identify, and how would you implement them in terms of domain local, global, and universal groups?

2. The chef is very temperamental, and one of the guarantees that has been made is that no one but him will have access to the server folders that will contain his secret recipes. Using some or all of the following tools, explain how you would set up access and security on his folders.
   - Groups
   - User rights
   - Attributes
   - Permissions
3. The table servers need access to two shared folders that will enable them to place orders from any of the seven workstations available to them. Explain how you would set up security on their folders.
4. The two business management staff need training in how to set up shared folders with access permissions and share permission security. Develop a set of instructions to help them understand how to set these up.
5. Once all of the new restaurants are in operation, Feasters wants to have a Web site from which to advertise services and take reservations. As preparation, explain to the two business management staff how to set up and manage Web sharing.
6. The owner and management staff use portable computers to connect to the network. Is there a way for them to take files from certain folders to work on at home and then easily update their work on the server the next day? If so, how?

## Optional Case Projects for Teams


### Team Case One

Mark Arnez is aware that certain customers of Aspen Consulting seem to run into trouble when configuring permissions, share permissions, and Web-share permissions. He is asking you to form a team that will develop a general document that explains how to resolve common permission conflicts.


### Team Case Two

Mark Arnez also wants to develop a comprehensive list of all of the ways in which group policies affect setup in a domain. Using the same group that you formed in Team Case One, develop a list of the ways in which group policies are used.